Capítulo 4
Active Directory Services

1. Introducción

Durante este capítulo Usted irá asimilando conocimientos acerca de los servicios de directorio (Active Directory Services) de Windows Server 2003, en particular, sobre algunas características nuevas de este servicio.

Para el desarrollo de las prácticas contenidas en esa unidad, necesitará la instalación de Windows Server 2003 realizada en la práctica 1 del capítulo 2 y una instalación adicional.

Al finalizar este capítulo Usted tendrá las habilidades de:

- Describir las características del servicio de directorio Active Directory.
- Identificar estructuras lógicas y físicas.
- Instalar y configurar Active Directory en la red.
- Identificar características referentes a la replicación.
- Solucionar problemas de Active Directory.

1.1. Definición

En una red de Microsoft® Windows® Server 2003, el servicio de directorio Active Directory® proporciona la estructura y las funciones para organizar, administrar y controlar el acceso a los recursos de red. Para implementar y administrar una red de Windows Server 2003, deberá comprender el propósito y la estructura de Active Directory.

Active Directory proporciona también la capacidad de administrar centralmente la red de Windows Server 2003. Esta capacidad significa que puede almacenar centralmente información acerca de la empresa, por ejemplo, información de usuarios, grupos e impresoras, y que los administradores pueden administrar la red desde una sola ubicación.

Active Directory admite la delegación del control administrativo sobre los objetos de él mismo. Esta delegación permite que los administradores asignen a un grupo determinado de administradores, permisos administrativosespecíficos para objetos, como cuentas de usuario o de grupo.

Active Directory es el servicio de directorio de una red de Windows Server 2003, mientras que un ***servicio de directorio*** es aquel que almacena información acerca de los recursos de la red y permite que los mismos resulten accesibles a los usuarios y a las aplicaciones. Los servicios de directorio proporcionan una manera coherente de nombrar, describir, localizar, tener acceso, administrar yasegurar la información relativa a los recursos de red.

1.2. La funcionalidad

Active Directory proporciona funcionalidad de servicio de directorio, como medio para organizar, administrar y controlar centralmente el acceso a los recursos de red. Asimismo hace que la topología física de red y los protocolos pasen desapercibidos, de manera que un usuario de una red pueda tener acceso a cualquier recurso sin saber dónde está el mismo o cómo está conectado físicamente a la red. Un ejemplo de este tipo de recurso es una impresora.

Active Directory está organizado en secciones que permiten el almacenamiento de una gran cantidad de objetos. Como resultado, es posible ampliar Active Directory a medida que crece una organización, permitiendo que una organización que tenga un único servidor con unos cuantos centenares de objetos, crezca hasta tener miles de servidores y millones de objetos.

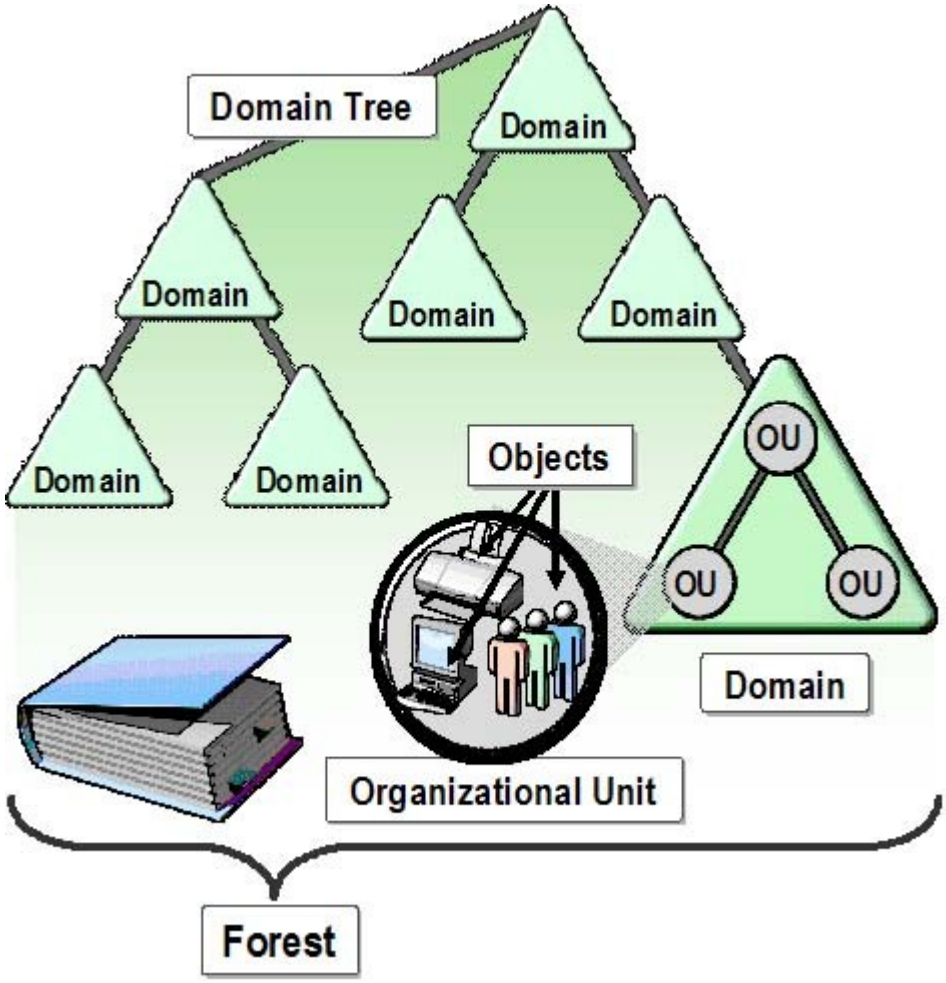
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Un servidor que ejecuta Windows Server 2003 almacena la configuración del sistema, la información de las aplicaciones y la información acerca de la ubicación de los perfiles de usuario en Active Directory. En combinación con las directivas de grupo, Active Directory permite a los administradores controlar escritorios distribuidos, servicios de red y aplicaciones desde una ubicación central, al tiempo que utiliza una interfaz de administración coherente.

Además, Active Directory proporciona un control centralizado del acceso a los recursos de red, al permitir que los usuarios sólo inicien sesión una sola vez para obtener pleno acceso a los recursos mediante Active Directory.

1.3. Estructura Lógica de Active Directory



Active Directory proporciona el almacenamiento seguro de la información sobre objetos en su estructura jerárquica lógica. Los objetos de Active Directory representan usuarios y recursos, como por ejemplo, las computadoras y las impresoras. Algunos objetos pueden llegar a ser containers para otros objetos.

Entendiendo el propósito y la función de estos objetos, Usted podrá realizar una variedad de tareas, incluyendo la instalación, la configuración, la administración y la resolución de problemas de Active Directory.

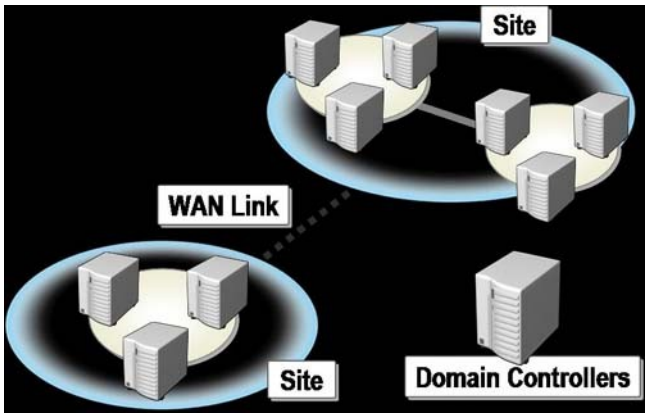
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

La estructura lógica de Active Directory incluye los siguientes componentes:

- ***Objects.*** Estos son los componentes básicos de la estructura lógica.
- ***Object classes.*** Son las plantillas o los modelos para los tipos de objetos que se pueden crear en Active Directory. Cada clase de objeto es definida por un grupo de atributos, los cuales definen los valores posibles que se pueden asociar a un objeto. Cada objeto tiene una combinación única de los valores de atributos.
- ***Organizational units.*** Usted puede utilizar estos container objects para organizar otros objetos con propósitos administrativos. Organizando objetos en Organizational Unit, se hace más fácil localizar y administrar objetos. Usted puede también delegar la autoridad para administrar las Organizational Unit. Estas últimas pueden contener otras Organizational Units para simplificar la administración de objetos.
- ***Domains.*** Son las unidades funcionales core de la estructura lógica de Active Directory, y asimismo es una colección de los objetos administrativos definidos, que comparten en una base de datos común del directorio, políticas de la seguridad y relaciones de confianza con otros Domains. Los Domains proporcionan las tres funciones siguientes:
  - Un límite administrativo para los objetos
  - Medios de administrar la seguridad para los recursos compartidos
  - Una unidad de réplica para los objetos
- ***Domain trees.*** Son Domains agrupados en estructuras de jerarquía. Cuando se agrega un segundo dominio a un tree, se convierte en Child del tree Root Domain. El dominio al cual un Child Domain se une, se llama Parent Domain. El Child Domain puede tener sus propios Child Domain, y su nombre se combina con el nombre de su Parent Domain para formar su propio y único nombre, Domain Name System (DNS). Un ejemplo de ellos sería corp.nwtraders.msft. De este modo, un tree tiene un Namespace contiguo.
- ***Forests.*** Un Forest es una instancia completa de Active Directory, y consiste en uno o más trees. En un solo two-level tree, el cual se recomienda para la mayoría de las organizaciones, todos los Child Domains se hacen Children del Forest Root Domain para formar un tree contiguo. El primer dominio en el forest se llama Forest Root Domain, y el nombre de ese dominio se refiere al forest, por ejemplo, nwtraders.msft. Por defecto, la información en Active Directory se comparte solamente dentro del forest. De esta manera, la seguridad del forest estará contenida en una sola instancia de Active Directory.

1.4. La estructura física de Active Directory



En contraste con la estructura lógica y los requisitos administrativos de los modelos, la estructura física de Active Directory optimiza el tráfico de la red, determinando cómo y cuándo ocurre la replicación y el tráfico de logon. Para optimizar el uso del ancho de banda de la red Active Directory, Usted debe entender la estructura física del mismo.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Los elementos de la estructura física de Active Directory son:

- ***Domain controllers.*** Estas computadoras corren Microsoft® Windows® Server 2003 o Windows 2000 Server y Active Directory. Cada Domain Controller realiza funciones de almacenamiento y replicación, y además soporta solamente un domain. Para asegurar una disponibilidad contínua de Active Directory, cada domain debe tener más de un Domain Controller.

- ***Active Directory sites.*** Los sites son grupos de computadoras conectadas. Cuando Usted establece sites, los Domain Controllers que están dentro de un solo site pueden comunicarse con frecuencia. Esta comunicación reduce al mínimo el estado de la latencia dentro del site, esto es, el tiempo requerido para un cambio que se realice en un Domain Controller y sea replicado a otros domain controllers. Usted crea sites para optimizar el uso del ancho de banda entre domain controllers en diversas locaciones.

- ***Active Directory partitions.*** Cada Domain Controller contiene las siguientes particiones de Active Directory:

    - Domain Partition, que contiene la réplica de todos los objetos en ese domain. Esta partición es replicada solamente a otros Domain Controllers en el mismo domain.

    - Configuration Partition, que contiene la topologia del forest. La topología registra todas las conexiones de los Domain Controllers en el mismo forest.

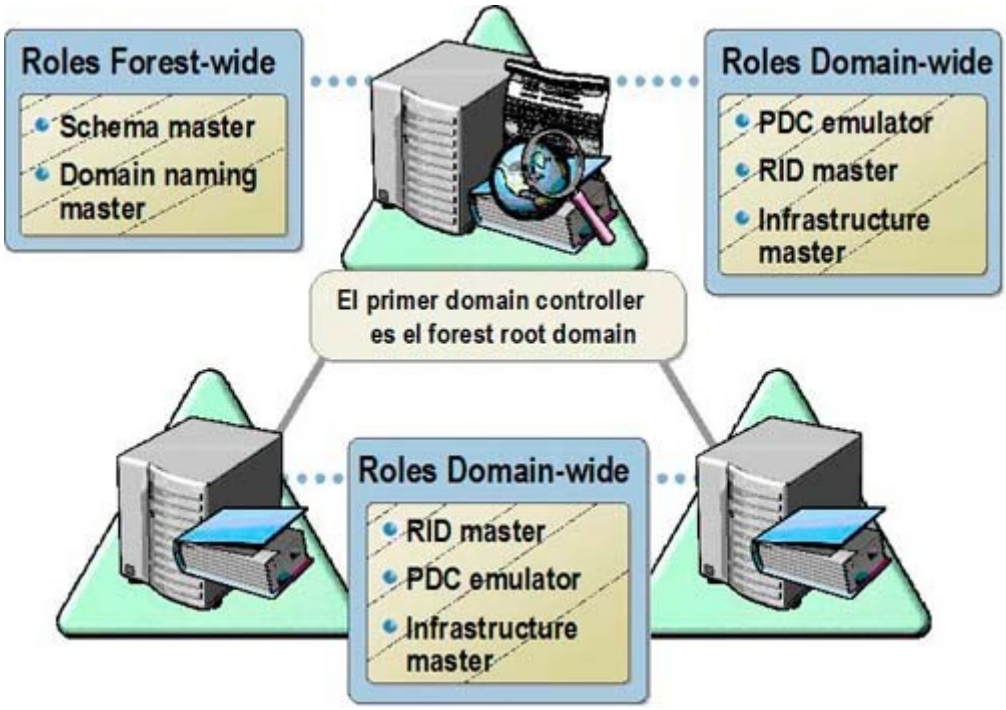
    - Schema Partition, que contiene el schema del forest. Cada forest tiene un schema de modo que la definición de cada clase del objeto sea constante. Las particiones Configuration y Schema Partitions son replicadas a cada Domain Controller en el forest.

- Application Partitions Ppcionales. que contienen los objetos relacionados a la seguridad y son utilizados por una o más aplicaciones. Las Application Partitions son replicadas a Domain Controllers específicos en el forest.

1.5. ¿Qué son los Operations Masters?

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by



Cuando un cambio se realiza a un domain, el cambio se replica a todos los Domain Controllers del mismo. Algunos cambios, por ejemplo los que se hacen en el schema, son replicados a todos los domains en el forest. Este tipo de replicación es llamada ***Multimaster Replication***.

1.5.1. Operaciones Single Master

Durante la replicación multimaster, puede ocurrir un conflicto de réplica donde se originen actualizaciones concurrentes en el mismo atributo del objeto y en dos Domain Controllers. Para evitar conflictos de réplica, Usted puede utilizar **Single Master Replication**, la cual asigna un Domain Controller como el único y en el que se pueden realizar cambios de directorio.

De esta manera, los cambios no pueden ocurrir en diversos lugares de la red al mismo tiempo. Active Directory usa Single Master Replication para los cambios importantes, por ejemplo, la adición de un nuevo domain o cambios al schema del forest.

1.5.2. Operations Master Roles

Las operaciones que utilizan Single Master Replication van junto a roles específicos en el forest o en el domain. Estos roles se llaman ***Operations Master Roles***. Para cada Operation Master Role, solamente el Domain Controller que tiene el rol puede realizar los cambios asociados al directorio. El Domain Controller que es responsable de un rol en particular se llama Operations ***Master para ese rol***. Active Directory, por su parte, almacena la información sobre el Domain Controller que cumple un rol especifico.

Los Operations Master Roles son a nivel forest o nivel domain, y Active Directory define cinco de ellos, los cuales tienen una localización por defecto.

Roles Forest-wide. Únicos en el forest, los roles forest-wide son:

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

- ***Schema master.*** Controla todas las actualizaciones al schema. El schema contiene la definición de clases de objetos y atributos que se utilizan para crear todos los objetos de Active Directory, como usuarios, computadoras, e impresoras.

- ***Domain Naming Master.*** Controla la adición o el retiro de domains en el forest. Cuando se agrega un nuevo domain al forest, solamente el Domain Controller que tenga el rol Domain Naming Master, podrá agregar el nuevo domain. Hay solamente un Schema Master y un Domain Naming Master por forest.

Roles Domain-wide. Para cada domain en el forest, los roles domain-wide son:

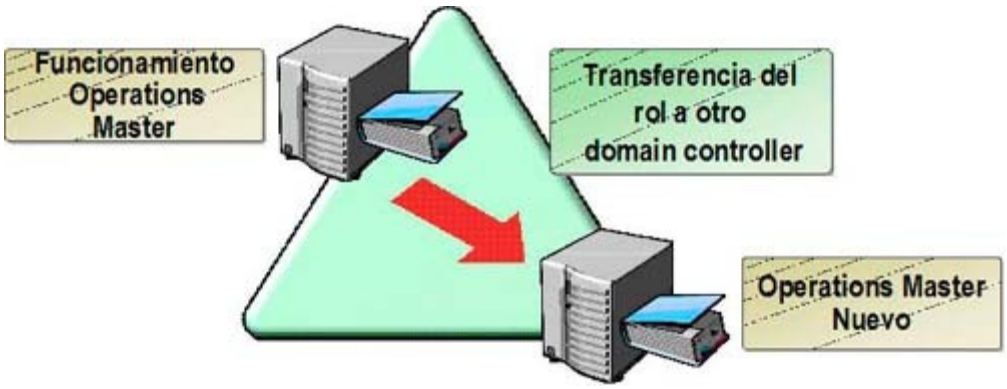
- ***Primary domain controller emulator (PDC).*** Actúa como un PDC Windows NT para soportar a los Backup Domain Controllers (BDCs) que corren Microsoft Windows® NT en domains, de modo mixto. Este tipo de domain tiene Domain Controller corriendo Windows NT 4.0. El PDC Emulator es el primer Domain Controller que se crea en un nuevo domain.

- ***Relative identifier master.*** Cuando se crea un nuevo objeto, el Domain Controller crea un nuevo Security Principal, que representa al objeto, asignándole un Unique Security Identifier (SID). El SID consiste en un Domain SID, que es igual para todos los Security Principals creados en el domain, y un relative identifier (RID), el cual es único para cada security principal creado en el domain. El RID Master asigna bloques de RIDs a cada Domain Controller en el domain. El Domain Controller entonces asigna el RID a los objetos se crean del bloque asignado de RIDs.

- ***Infrastructure master.*** Cuando los objetos se mueven de un domain a otro, el Infrastructure Master actualiza las referencias al objeto en ese domain y la referencia al objeto en el otro dominio. La referencia del objeto contiene el Object Globally Unique Identifier (GUID), el Distinguished Name y el SID. Active Directory actualiza periódicamente el Distinguished Name y el SID, en la referencia al objeto para reflejar los cambios realizados en el objeto real, por ejemplo, movimientos en y entre domains o la eliminación del objeto.

Cada domain en el forest tiene su propio PDC Emulator, RID Master e Infrastructure Master.

1.5.3. Transferencia de Operations Master Roles



Usted colocará los Operations Master Roles en un forest cuando implemente una estructura de forest y dominio. Los Oerations Master Roles se transfieren, solamente cuando se realiza un cambio importante en la infraestructura del dominio. Tales cambios incluyen el desarme de un Domain Controller que haya tenido un rol, y la adición de un nuevo Domain Controller que satisfaga mejor las operaciones de un rol específico.

La transferencia de Operations Master Roles implica mover el rol de un Domain Controller a otro. Para transferir roles, los dos Domain Controllers deben estar funcionando y conectados a la red.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Ninguna pérdida de datos ocurre cuando Usted transfiere Operations Master Role. Active Directory replica el actual Operation Master Role al nuevo Domain Controller, asegurando que el nuevo Operation Master Role obtendrá la información necesaria para dicho rol. Esta transferencia utiliza el mecanismo de la réplica del directorio.

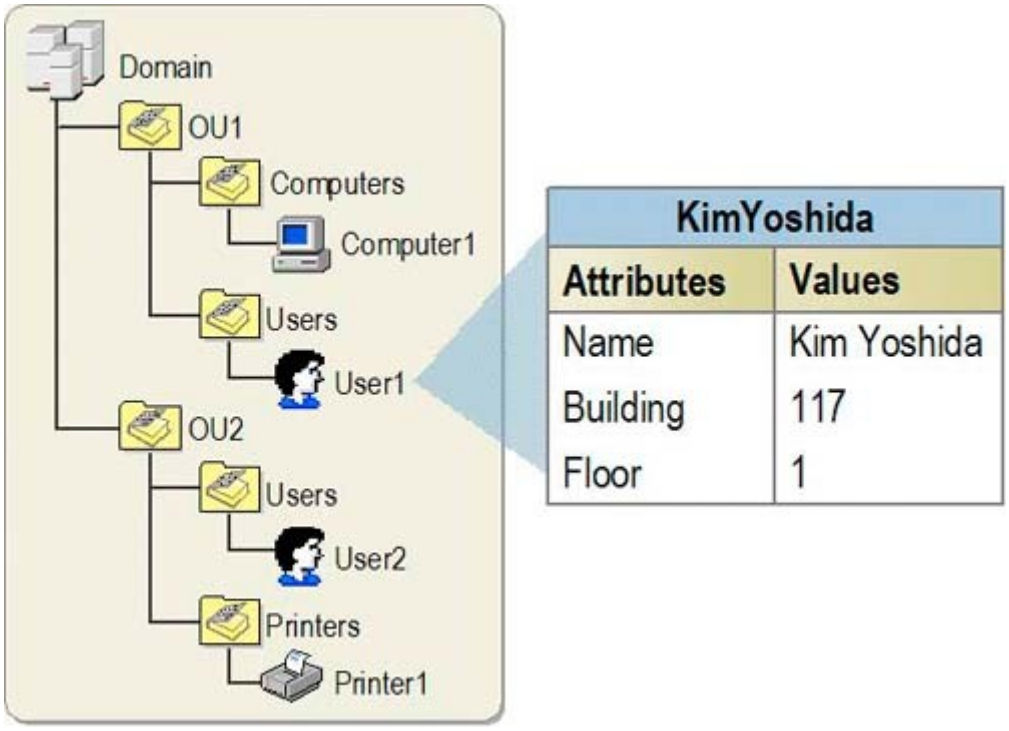
Para obtener información sobre el proceso de transferencia:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324801

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2. ¿Qué es el servicio de directorio?



Un servicio de directorio es un depósito estructurado de la información sobre personas y recursos en una organización. En una red Windows Server 2003, el servicio de directorio es Active Directory.

2.1. Active Directory tiene las siguientes capacidades:

- ***Permite a usuarios y aplicaciones tener acceso a la información sobre objetos.*** Esta información se almacena en forma de valores atributos. Usted buscará objetos basándose en su clase, atributo, valor del atributo, localización dentro de la estructura de Active Directory, o cualquier combinación de estos valores.

- ***Hace transparentes la topología y los protocolos físicos de la red.*** De esta manera, un usuario en una red puede tener acceso a cualquier recurso, por ejemplo a una impresora, sin saber dónde está el recurso o dónde está conectado físicamente con la red.
  o Permite el almacenamiento de un número muy grande de objetos. Dado que se organiza en particiones, Active Directory puede ampliarse mientras que una organización crece. Por ejemplo, un directorio puede ampliarse de un solo servidor con algunos objetos a millares de servidores y millones de objetos.

- new! ***Puede funcionar como servicio Non-Operating System.*** Active Directory in Application Mode (AD/AM) es una nueva capacidad de Microsoft Active Directory y actúa en escenarios de aplicaciones Directory-Enabled. AD/AM funciona como servicio Non-Operating System que, como tal, no requiere instalación sobre un Domain Controller. Correr servicios Non-Operating System significa que múltiples instancias de AD/AM pueden funcionar concurrentemente en un solo servidor, siendo cada instancia independientemente configurable.

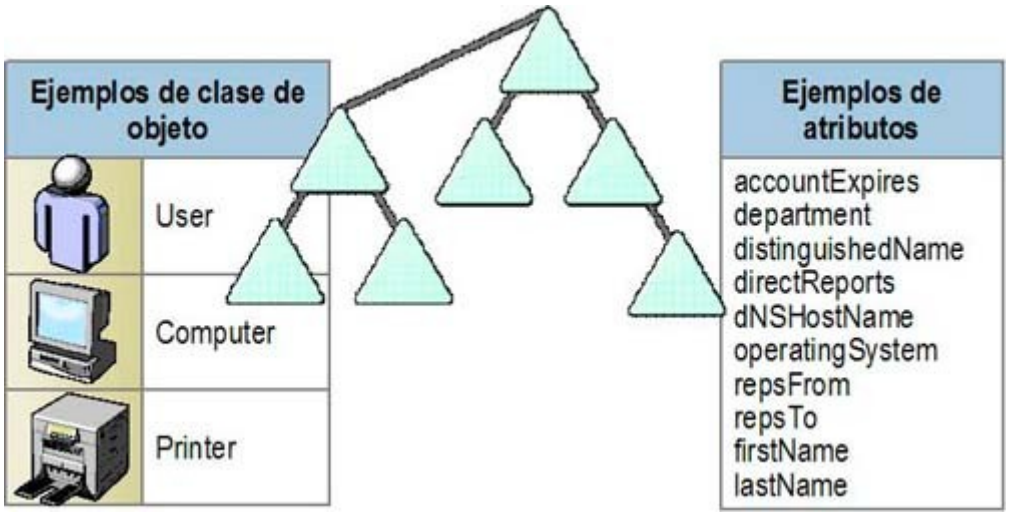
Para obtener más información acerca de ADAM (Active Directory Aplication Mode):

http://www.microsoft.com/windowsserver2003/techinfo/overview/adam.mspx

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.2. ¿Qué es el Schema?



El Schema de Active Directory contiene las definiciones de todos los objetos, como por ejemplo usuarios, computadoras e impresoras almacenados en Active Directory. Sobre Domain Controllers corriendo Windows Server 2003, hay solamente un Schema para todo el forest. De esta manera, todos los objetos que se crean en Active Directory cumplen con las mismas reglas.

El Schema tiene dos tipos de definiciones: Object Classes y atributos. Un ejemplo de Object Classes son los usuarios, la computadora y la impresora, que describen los objetos posibles que se pueden crear en el directorio. Cada Object Class es una colección de atributos. Los atributos se definen separadamente de los Object Classes. Cada atributo se define solamente una vez y puede ser utilizado en múltiples Object Classes. Por ejemplo, el atributo de la descripción se utiliza en muchos Object Classes, pero se define solamente una vez en el Schema para asegurar consistencia.

Asimismo Usted puede crear nuevos tipos de objetos en Active Directory extendiendo el Schema. Por ejemplo, para un aplicación E-mail Server, se podría ampliar el User Class en Active Directory con nuevos atributos que contengan información adicional, como la dirección y el e-mail de los usuarios.

new! Sobre Domain Controllers Windows Server 2003, Usted puede revertir cambios al Schema desactivándolos y permitiendo a las organizaciones, de esta forma, mejorar el uso de las características de extensibilidad de Active Directory.

new! También se puede redefinir una clase o atributo del Schema, por ejemplo, cambiar la sintaxis de la secuencia de Unicode del atributo llamado SalesManager a Distinguished Name.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.3 ¿Qué es el Global Catalog?

El ***global Catalog*** es un repositorio de información que contiene un subconjunto de atributos de todos los objetos en Active Directory. Los miembros del grupo Schema Admins pueden cambiar los atributosque son almacenados en el Global Catalog, dependiendo de los requerimientos de la organización.

El Global Catalog contiene:

- Los atributos que se utilizan con más frecuencia en queries, por ejemplo, first name, last name y logon name de los usuarios.
- La información que es necesaria para determinar la localización de cualquier objeto en el directorio.
- Un subconjunto por defecto de los atributos para cada tipo de objeto.
- Los permisos de acceso para cada objeto y atributos, que son almacenados en el Global Catalog. Si Usted busca un objeto y no tiene los permisos apropiados para verlo, el objeto no aparecerá en los resultados de la búsqueda. Los permisos de acceso aseguran que los usuarios puedan encontrar solamente los objetos a los cuales les han asignado el acceso.

El ***Global Catalog Server*** es un Domain Controller que procesa eficientemente queries intraforest al Global Catalog. El primer Domain Controller que Usted crea en Active Directory se convierte automáticamente en Global Catalog Server. Usted puede configurar Global Catalog Servers adicionales para balancear el tráfico para logon y queries.

El Global Catalog permite a usuarios realizar dos funciones importantes:

- Buscar información en Active Directory en todo el forest, sin importar la localización de los datos.
- Usar información del membership del Universal Group en el proceso de logon a la red.

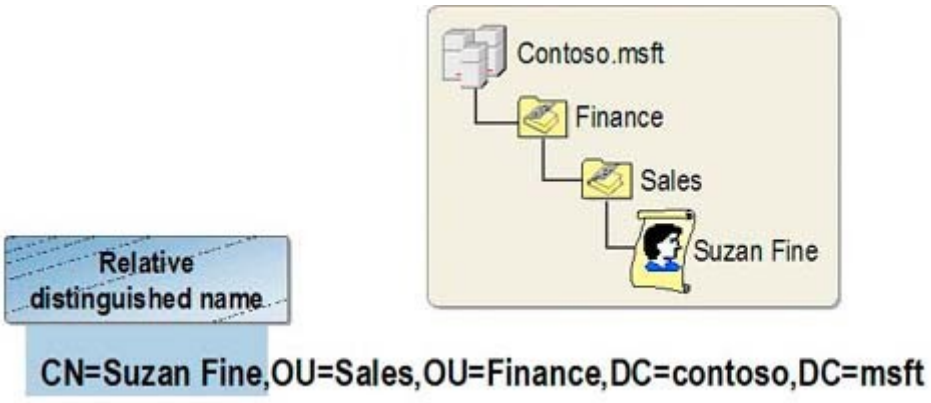
new! Los Global Catalog Servers replican su contenido en un esquema de replicación. Hasta Windows 2000 estas réplicas eran del tipo full sync, pero a partir de Windows Server 2003 se hacen de modo partial sync, es decir, solo se replican cambios en lugar de enviar el catalogo completo.

new! Para poder utilizar esta nueva característica de Windows Server 2003, Usted puede tener el nivel funcional del forest en modo Windows 2000 o Windows server 2003, pero solamente se harán réplicas parciales entre los servidores Global Catalog que corran Windows Server 2003.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

2.4 ¿Qué son los Distinguished y Relative Distinguished Names?



LDAP utiliza un nombre que representa objetos en Active Directory por una serie de componentes que se relacionan con la estructura lógica. Esta representación es llamada ***Distinguished Name*** del objeto, e identifica el domain donde se localiza el objeto y la trayectoria completa por la cual el objeto es alcanzado. El Distinguished Name debe ser único en el Active Directory forest.

El ***Relative Distinguished Name*** de un objeto identifica únicamente el objeto en su container. Dos objetos en el mismo container no pueden tener el mismo nombre. El Relative Distinguished Name siempre es el primer componente del Distinguished Name, pero puede no ser siempre un Common Name.

Para un usuario llamado Suzan Fine de Sales Organizational Unit en Contoso.msft domain, cada elemento de la estructura lógica se representa en el siguiente Distinguished Name:

CN=Suzan Fine,OU=Sales,DC=contoso,DC=msft

- CN es el Common Name del objeto en su container.
- OU es la Organizational Unit que contiene el objeto. Puede haber más de un valor de OU si el objeto reside en una Organizational Unit anidada a más niveles.
- DC es el Domain Component, por ejemplo .com. o .msft.. Hay siempre al menos dos Domain Components, pero posiblemente más si el domain es un child domain.

Los domain components de los Distinguished Name están basados en Domain Name System (DNS).

2.5. Active Directory Snap-ins y Herramientas

Windows Server 2003 proporciona un número de snap-ins y herramientas command-line para administrar Active Directory. Usted puede también administrar Active Directory usando Active Directory Service Interfaces (ADSI). ADSI es una interfaz simple de gran alcance para crear scripts reutilizables para administrar Active Directory.

Nota: La herramienta ADSI Edit puede instalarse, desde el CD de Windows Server 2003. La misma se encuentra en la carpeta \Support\Tools.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

La tabla siguiente describe los snap-ins administrativos comunes para administración de Active Directory.

Snap-in	Descripción
Active Directory Users and Computers	Es una Microsoft Management Console (MMC) que se utiliza para administrar y publicar la información en Active Directory. Usted puede administrar cuentas de usuario, grupos, y cuentas de computadora, agregar computadoras al domain, administrar políticas de cuentas, derechos de usuario, y políticas de auditoria.
Active Directory Domains and Trusts	Es una MMC que se utiliza para administrar Domain Trusts y Forest Trusts, agregar sufijos user principal name, y cambiar niveles de funcionamiento de domains y forest. Active Directory Sites and Services Es una MMC que usted utiliza para administrar replicacion de directorio.
Active Directory Schema	Es una MMC que se utiliza para administrar el Schema. No está disponible por defecto en el menu
Administrative Tools.	Usted debe agregarlo manualmente.

La tabla siguiente describe las herramientas de command-line para utilizar cuando se quiera administrar Active Directory.

Herramienta	Descripción
Dsadd	Agrega objetos a Active Directory, tales como computadoras, usuarios, grupos, organizational units y contactos.
Dsmod	Modifica objetos en active Directory, tales como computadoras, servidores, usuarios, grupos, organizational units y contactos.
Dsquery	Corre queries en Active Directory según criterios especificados. Usted puede correr queries contra servidores, computadoras, grupos, usuarios, sites, organizational units, y particiones.
Dsmove	Mueve objetos dentro de un dominio, a una nueva localización en Active Directory o renombra un solo objeto sin moverlo.
Dsrm	Suprime un objeto de Active Directory.
Dsget	Muestra atributos seleccionados de una computadora, contacto, grupo, organizational unit, servidor o usuario de Active Directory.
Csvde	Importa y exporta datos de Active Directory usando formato separado por comas.
Ldifde	Crea, modifica y borra objetos de Active Directory. Puede también extender el Schema de Active Directory y exportar información de usuarios y grupos a otras aplicaciones o servicios.

Para obtener más información acerca de las herramientas command-line:

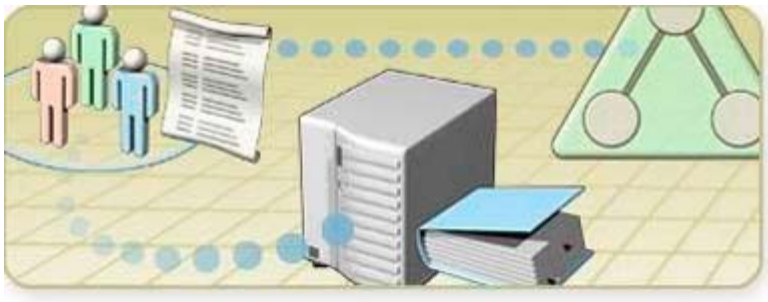
http://support.microsoft.com/default.aspx?scid=kb;en-us;322684

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3. Instalación de Active Directory

3.1. Requisitos para instalar Active Directory



Antes de instalar Active Directory, Usted debe asegurarse que la computadora esté configurada como Domain Controller, cumpliendo con los requisitos de hardware y del sistema operativo. Además, el Domain Controller deberá tener acceso al DNS Server, que deberá cumplir con ciertos requisitos para soportar la integración con Active Directory.

La lista siguiente identifica los requisitos para la instalación de Active Directory:

- Una computadora corriendo Microsoft® Windows® Server 2003 Standard Edition, Enterprise Edition o Datacenter Edition. Windows Server 2003 Web Edition no soporta Active Directory.

- Un mínimo de 250 megabytes (MB) de espacio en disco.200 MB para la base de datos de Active Directory y 50 MB para logs de transacciones de Active Directory. Los requisitos de tamaño del archivo para la base de Active Directory y los archivos log, dependen del número y el tipo de objetos en el domain. Se requerirá el espacio de disco adicional si el Domain Controller también es Global Catalog Server.

- Una partición o un volumen con formato NTFS y con sistema de archivos. La partición NTFS se requiere para la carpeta SYSVOL.

- Los privilegios administrativos necesarios para crear un domain, si es que Usted está creando uno en una red existente Windows Server 2003.

- TCP/IP instalado y configurado para utilizar DNS.

- Un DNS Server autoritativo para el DNS Domain y soporte para los requisitos enumerados en la siguiente tabla.

- ***SRV Resource Records (Mandatory) Service Locator Resource (SRV).*** Son registros DNS que identifican los servicios específicos que ofrecen las computadoras en una red Windows Server 2003. El DNS Server que soporta la instalación de Active Directory necesita soporte de SRV Resource Records. De lo contrario, Usted deberá configurar el DNS localmente durante la instalación de Active Directory o configurar el DNS manualmente después de la instalación de Active Directory.

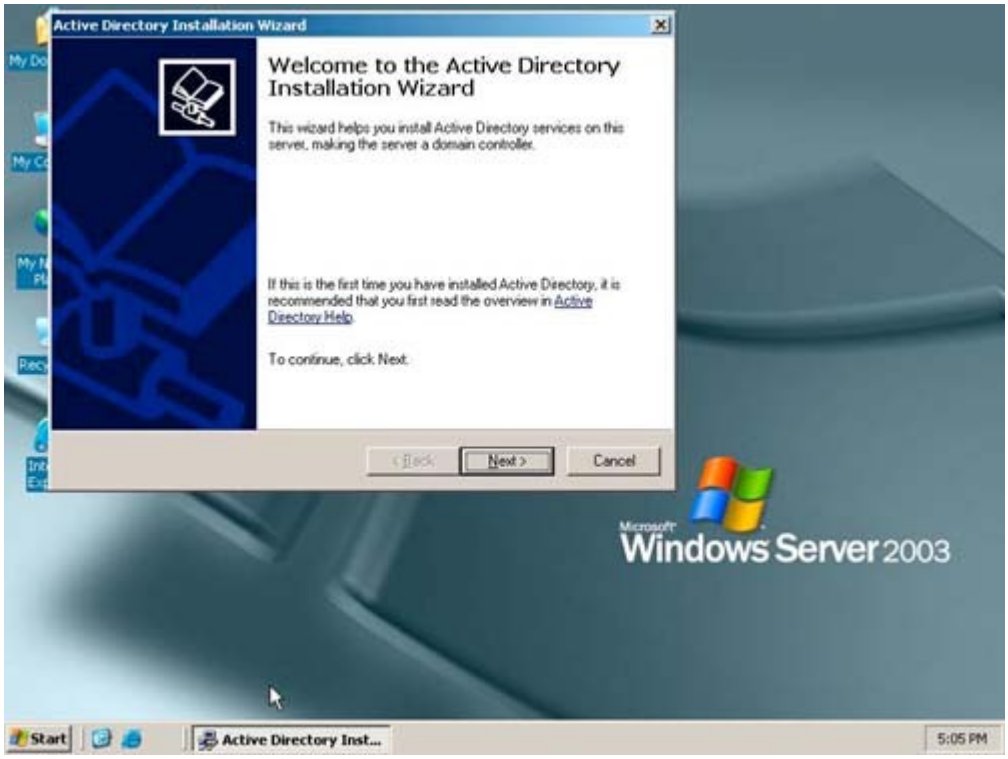
- ***Dynamic Updates (Opcional).*** Microsoft recomienda que los servidores DNS también soporten actualizaciones dinámicas. El protocolo dinámico de actualización permite a los servidores y a los clientes, en un ambiente DNS, agregar y actualizar la base de datos del DNS automáticamente, lo que reduce esfuerzos administrativos. Si Usted utiliza software DNS que soporta SRV Resource Records pero que no soporta el protocolo dinámico de actualización, deberá ingresar los SRV Resource Records manualmente en la base DNS.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

- ***Incremental Zone Transfers (Opcional).*** En una transferencia incremental de zona, los cambios realizados en una zona en el Master DNS Server, deben ser replicados a los DNS Servers secundarios de esa zona. Las transferencias incrementales de la zona son opcionales, pero se recomiendan porque ahorran ancho de banda de la red, replicando solamente los registros nuevos o modificados entre los DNS Servers, en vez del archivo de base de datos entero de la zona.

3.2 El proceso de instalación de Active Directory



El proceso de la instalación realiza las siguientes tareas:

- ***Inicia el protocolo de autenticación Kerberos version 5***

- ***Aplica la politica Local Security Authority (LSA).*** Esta configuración indica que el server es un Domain Controller.

- ***Crea las particiones de Active Directory.*** Una partición del directorio es una porción del Directory Namespace. Cada partición del directorio contiene una jerarquía o subtree de los objetos del directorio en el árbol del directorio. Durante la instalación, se crean las particiones siguientes en el primer domain controller del forest:

  - Schema Directory Partition
  - Configuration Directory Partition
  - Domain Directory Partition
  - Forest DNS Zone
  - Domain DNS Zone Partition

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Las particiones, entonces, se actualizarán a través de la réplica, en cada uno de los Domain Controllers creados subsiguientemente en el forest.

- ***Crea la base de datos y los logs de Active Directory.*** La locación por defecto para la base de datos y los archivos de logs es systemroot\Ntds.

- ***Crea el forest root domain.*** Si el servidor es el primer Domain Controller en la red, el proceso de la instalación crea el Forest Root Domain, y entonces le asignará los Operations Master Roles al Domain Controller, incluyendo:

    - Primary Domain Controller (PDC) Emulator
    - Relative Identifier (RID) Operations Master
    - Domain-Naming Master
    - Schema Master
    - Infrastructure Master

- ***Crea la carpeta compartida del volumen del sistema.*** Esta estructura de carpetas reside en todos los Windows Server 2003 Domain Controllers y contiene las siguientes carpetas:

- La carpeta compartida SYSVOL, que contiene información de Group Policy.
- La carpeta compartida Net Logon, que contiene los logon scripts para computadoras que no corren Windows Server 2003.

- ***Configura pertenencia al site apropiado para el Domain Controller.*** Si la IP del servidor que Usted está promoviendo a Domain Controller está dentro de una subnet definida en Active Directory, el wizard colocará el Domain Controller en el site asociado con la subnet. Si no se define ningún objeto de subnet o si la IP del servidor no está dentro del rango de la subnet presente en Active Directory, el servidor se colocará en el site Default-First-Site-Name. El primer site se instala automáticamente cuando Usted crea el primer Domain Controller en el forest. El wizard de instalación de Active Directory crea un objeto servidor del Domain Controller en el site apropiado. El objeto servidor contiene la información requerida para la réplica y asimismo contiene una referencia al objeto de la computadora en la OU Domain Controllers, representando que el Domain Controller está siendo creado.

- ***Permite seguridad en el Directory Service y en File Replication Folders.*** Esto implica controlar el acceso de usuario a objetos de Active Directory Objects.

- ***Aplica el password para la cuenta del administrador.*** Usted utiliza la cuenta para iniciar el Domain Controller en Directory Services Restore Mode.

3.2.1. Practica 1: ¿Cómo crear la estructura del Forest y el Domain?

Usted utiliza Active Directory Installation Wizard para crear la estructura de forest y domain. Cuando instale Active Directory por primera vez en una red, tendrá que crear el Forest Root Domain, y después de ello utilizar el wizard para crear trees y Child Domains adicionales.

El Active Directory Installation Wizard guíará a Usted en el proceso de la instalación y le solicitará la información necesaria, la varía según las opciones que seleccione.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Para crear el Forest Root Domain, deberá realizar los siguientes pasos:

1. Hacer click en ***Start***, después en ***Run*** y escribir ***dcpromo***. Luego presionar Enter. El Wizard verificará:
   - Si el usuario actualmente validado es un miembro del grupo de administradores locales.
   - Si en la computadora está funcionando en un sistema operativo que soporte Active Directory.
   - Si una instalación o un retiro anterior de Active Directory no ha ocurrido sin reiniciar la computadora, o que una instalación o un retiro de Active Directory no está en marcha. Si cualesquiera de estas cuatro verificaciones fallan, un mensaje de error aparecerá y Usted saldrá del wizard.
2. En la página ***Welcome,*** hacer click en ***Next***.
3. En la página ***Operating System Compatibility***, hacer click en ***Next***.
4. En la página ***Domain Controller Type***, hacer click en ***Domain controller for a new domain***, y después hacer click en ***Next***.
5. En la página ***Create New Domain***, hacer click en Domain in a new forest, y después en ***Next***.
6. En la página ***New Domain Name***, ingresar el DNS Name para el nuevo domain (nwtraders.msft), y después hacer click en ***Next***.
7. En la página NetBIOS Domain Name, verificar NetBIOS Name (NWTRADERS), y después hacer click en Next.
   El nombre NetBIOS identifica el domain a las computadoras de cliente corriendo versiones anteriores de Windows y Windows NT. El wizard verifica que le nombre NetBIOS sea único. Si no lo es, le pedirá cambiar el nombre.
8. En la página ***Database and Log Folders***, especificar la localización en la cual se desea instalar las carpetas de la base de datos y de los logs. Después hacer click en ***Next***.
9. En la página ***Shared System Volume***, especificar la locación en la cual se desea instalar la carpeta de SYSVOL, o hacer click en ***Browse*** para elegir una locación, y después hacer click en ***Next***.
10. En la pagina ***DNS Registration Diagnostics***, verificar si un servidor existente de DNS es autoritario para este forest o, en caso de necesidad, hacer click en ***Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server***, y después hacer click en ***Next***.
11. En la pagina ***Permissions***, especificar se si asignan los permisos por defecto en los objetos usuario y grupo compatible con los servidores que funcionan con versiones anteriores de Windows o Windows NT, o solamente con los servidores Windows Server 2003.
12. Cuando se pregunte, especificar el password para Directory Services Restore Mode. Los Domain Controllers Windows Server 2003 mantienen una versión pequeña de la base de datos de cuentas de Microsoft Windows NT 4.0. La única cuenta en esta base de datos es la cuenta del administrador y la misma se requiere para la autentificación al encender la computadora en Directory Services Restore mode, porque Active Directory no se inicia de este modo.
13. Repasar la página ***Summary***, y después hacer click en ***Next*** para comenzar la instalación.
14. Cuando se pregunte, reiniciar la computadora.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

3.2.2 Práctica 2 (Opcional): ¿Cómo agregar un Domain Controller adicional?

Para llevar a cabo esta práctica Usted necesitará dos computadoras o dos Virtual PC, con un Domain Controller instalado (Práctica 1) y un Windows Server 2003.

El procedimiento es similar a la creación de un nuevo Domain Controller; solamente se debe seleccionar, en la primera pantalla del wizard, la opción ***Add additional Domain Controller for existing domain***. El resto del proceso se puede realizar de dos formas:

1. ***Over the network:*** Esto requiere, en el caso que Usted tenga gran cantidad de objetos, un enlace con ancho de banda suficiente o bastante tiempo para la replica inicial.
2. new! ***Replicate from Media:*** Esta nueva característica de Windows Server 2003, permite realizar la replica inicial por medio de un backup, de la siguiente manera:
   - Primero debe realizar un backup del System State en el Domain Controller existente.
   - Luego debe hacer llegar ese backup a la computadora destino.
   - En la computadora destino deberá realizar la operación de restore en una locación alternativa (Elija una carpeta ej: C:\NTDSRestore)
   - Por último corra el wizard ***dcpromo /adv***
   - El wizard le permitirá seleccionar la opción ***From Media***

3.3. new! ¿Cómo renombrar un Domain Controller?

En Windows Server 2003, Usted puede renombrar un Domain Controller después que haya sido instalado. Para renombrar un Domain Controller, deberá tener derechos de Domain Admin.

Cuando Usted renombre un Domain Controller, deberá agregar el nuevo nombre del Domain Controller y remover el nombre viejo de las bases de DNS y Active Directory. El renombrado de un Domain Controller es solamente posible si el Domain Functional Level es configurado como Windows Server 2003.

Para renombrar un Domain Controller, deberá realizar los siguientes pasos:

1. En Control Panel, hacer doble-click en ***System***.
2. En el cuadro ***System Properties***, en ***Computer Name***, hacer click ***Change***.
3. Cuando se pregunte, confirmar si se desea renombrar el Domain Controller.
4. Incorporar el nombre de computadora completo (incluyendo el primary DNS suffix), y después hacer click en ***OK***.

Usted podrá cambiar el Primary DNS suffix de un Domain Controller cuando renombre el Domain Controller. Sin embargo, el cambiar el Primary DNS suffix no mueve el Domain Controller a un nuevo Active Directory domain. Por ejemplo, si Usted renombra dc2.nwtraders.msft a dc1.contoso.msft, la computadora sigue siendo un Domain Controller del dominio nwtraders.msft, aunque su Primary DNS suffix es contoso.msft. Para mover un Domain Controller a otro domain, Usted debe primero degradar el Domain Controller y entonces promoverlo
en el nuevo dominio.

Obtenga información acerca de instalación de Active Directory:

http://support.microsoft.com/default.aspx?scid=kb;en-us;324753

http://support.microsoft.com/default.aspx?scid=kb;en-us;816106

http://support.microsoft.com/default.aspx?scid=kb;en-us;816108

http://support.microsoft.com/default.aspx?scid=kb;en-us;814589

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

3.4. ¿Cómo solucionar problemas en la instalación de Active Directory?

Al instalar Active Directory, Usted puede encontrar problemas. Éstos pueden ser credenciales incorrectas de seguridad, el uso de nombres que no son únicos, una red no fiable o recursos escasos.

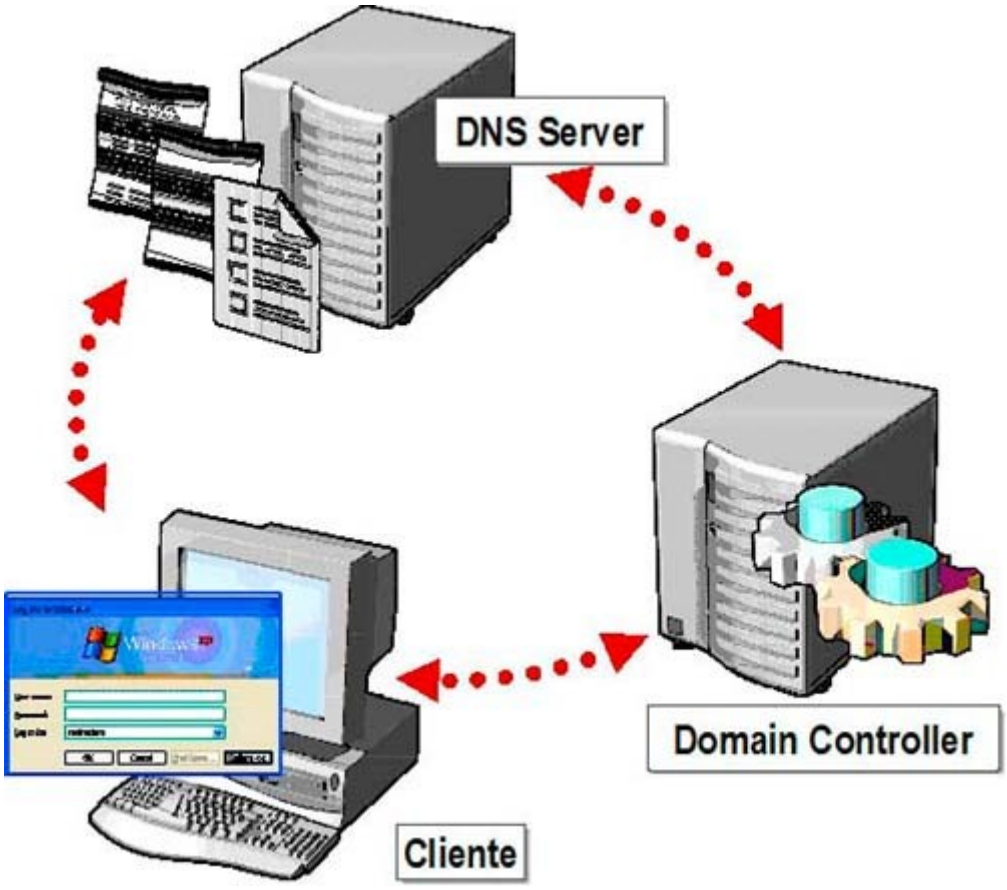
A continuación se describen algunos problemas comunes que Usted puede llegar a encontrar mientras instala Active Directory, y algunas estrategias para resolverlos.

Tener acceso negado mientras que crea o agrega Domain Controllers. Cerrar la sesión y después iniciar con una cuenta que pertenezca al grupo local de administradores. Las credenciales deben ser de un usuario que sea miembro de Domain Admins o Enterprise Admins.

El nombre DNS o NetBIOS del domain no es único Cambiar el nombre a un nombre único.

El domain no puede ser contactado Comprobar que haya conectividad de red entre el servidor que Usted está promoviendo a Domain Controller y que por lo menos haya un Domain Controller en el dominio. Utilizar el comando ping desde command prompt para probar la conectividad con cualquier Domain Controller del dominio. Verificar que el DNS proporcione la resolución de nombres, por lo menos a un Domain Controller en el dominio.

4. ¿Qué son las zonas DNS Active Directory Integrated?



© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

4.1. Introducción

Una ventaja de integrar el DNS y Active Directory es la capacidad de integrar zonas de DNS en la base de datos de Active Directory. Una zona es una porción del Domain Namespace, que agrupa registros lógicamente, permitiendo transferencias de zona de éstos registros para funcionar como una unidad.

4.2. Zonas Active Directory Integrated

Los Microsoft DNS Servers almacenan la información que es utilizada para resolver nombres de host a direcciones IP y direcciones IP a nombres de host, usando una base de datos en formato de archivo que tenga una extensión .dns para cada zona.

Las Zonas Active Directory Integrated son primarias y stub, y se almacenan como objetos en la base de Active Directory. Usted puede almacenar objetos de zona en Active Directory Application Partition o en Active Directory Domain Partition. Si los objetos de zona se almacenan en Active Directory Application Partition, solamente los Domain Controllers que suscriban a esa Application Partition pueden participar en la réplica de esta partición. Sin embargo, si los objetos de zona se almacenan en Active Directory Domain Partition, se replican a todos los Domain Controllers en el dominio.

4.3. Ventajas de Zonas Active Directory Integrated

Las Zonas Active Directory Integrated ofrecen las siguientes ventajas.

- ***Multimaster replication.*** Cuando Usted configura Zonas Active Directory Integrated, las actualizaciones dinámicas al DNS se basan en el modelo multimaster. En este modelo, cualquier servidor autoritativo DNS, por ejemplo un Domain Controller corriendo DNS Server, es primario para la zona. Dado que la Master Copy de la zona se mantiene en la base de Active Directory (la cual se replica completamente a todos Domain Controllers), la zona se puede actualizar por los DNS Servers funcionando en cualquier Domain Controller del dominio.

- ***Secure dynamic updates.*** Debido a que las zonas de DNS son objetos de Active Directory en Zonas Active Directory Integrated, Usted puede aplicar permisos a los registros dentro de esas zonas y también puede controlar qué computadoras pueden actualizar sus registros. De esta manera, las actualizaciones que utilizan el protocolo dinámico de actualización pueden venir solamente de las computadoras autorizadas.

Para obtener más información acerca de Zonas Active Directory Integrated:

http://support.microsoft.com/default.aspx?scid=kb;en-us;816101

4.4. Práctica 3: Verificación de Zona integrada con Active Directory

Durante esta práctica Usted verificará si su DNS Server, tiene la zona integrada con Active Directory.

Para verificar DNS:

1. Abrir la consola de DNS.
2. Hacer click en el nombre del server.
3. Hacer click en la zona a verificar.
4. Hacer click derecho en la zona, y después en ***Properties***.
5. En el cuadro ***zone type***, verificar ***Active Directory Integrated***
6. Para cambiar el tipo de zona, hacer click en ***Change***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

5. ¿Qué es la funcionalidad de Forest y Domain?

Ambiente de red	Domain functional levels	Forest functional levels
Windows 2000 mixed-mode domain	✓	
Windows 2000 native-mode domain	✓	✓
Windows Server 2003 Domain	✓	✓
Windows Server 2003 Interim	✓	

5.1. Introducción

En Windows Server 2003, la funcionalidad de forest y domain proporciona una manera de permitir características nuevas forest-wide o domain-wide de Active Directory en su ambiente de red. Diversos niveles de la funcionalidad del forest y del dominio están disponibles, dependiendo de su ambiente de red.

5.2. ¿Qué es la funcionalidad de dominio?

La funcionalidad del dominio habilita las características que afectarán el dominio entero y solamente ese dominio. Cuatro niveles funcionales de dominio están disponibles:

- ***Windows 2000 mixed.*** Éste es el nivel funcional por defecto. Usted puede levantar el nivel funcional del dominio a Windows 2000 native o Windows Server 2003. Los dominios Mixed-mode pueden contener Windows NT 4.0 backup Domain Controllers, pero no pueden utilizar grupos de seguridad universales, anidamiento de grupos o capacidades de Security Identifier (SID) History.
- ***Windows 2000 native.*** Usted puede utilizar este nivel funcional si el dominio contiene solamente Domain Controllers Windows 2000 y Windows Server 2003. Aunque los Domain Controllers funcionen en Windows 2000 Server, no están preparados para la funcionalidad de dominio. Características de Active Directory, como grupos de seguridad universales, anidamiento de grupos y capacidades de Security Identifier (SID) History, están disponibles.
- ***Windows 2003 Server.*** Este es el nivel funcional más alto para un dominio. Usted puede utilizarlo solamente si todos los Domain Controllers en el dominio funcionan en Windows Server 2003. Todas las características de Active Directory para el dominio están disponibles para su uso.
- new! ***Windows 2003 Interim.*** Este nivel es un nivel funcional especial que soporta Domain Controllers Windows NT 4.0 y Windows server 2003.

5.3. new! ¿Qué es la funcionalidad de forest?

La funcionalidad de forest habilita características a través de todos los dominios dentro de su forest. Dos niveles funcionales de forest están disponibles: Windows 2000 y Windows Server 2003. Por defecto, los forests funcionan en nivel funcional Windows 2000. Usted puede elevar el nivel funcional del forest a

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

Windows Server 2003, para que habilite las características que no están disponibles en el nivel funcional Windows 2000, incluyendo:

- Relaciones de confianza entre forest
- Replicación mejorada

Importante: Usted no puede bajar el nivel funcional del dominio o del forest después que se haya elevado.

5.4. new! Requisitos para habilitar nuevas características en Windows Server 2003

Requisito	Domain	Forest
Domain controllers corriendo:	Windows Server 2003	Windows Server 2003
El nivel funcional del dominio debe ser :	Elevado a Windows Server 2003	Capaz de ser elevado a Windows Server 2003
Administrator:	Administrador del dominio para elevar el nivel funcional del dominio	Enterprise administrator para elevar el nivel funcional del forest

5.4.1 new! Introducción

Además de las características básicas de Active Directory en Domain Controllers individuales, nuevas características forest-wide y domain-wide están disponibles cuando se cumplen ciertas condiciones.

Para habilitar las nuevas características domain-wide, todos los Domain Controllers en el dominio deben correr Windows Server 2003, y el nivel funcional del dominio se debe elevar a Windows Server 2003. Usted debe ser administrador del dominio para elevar el nivel funcional del dominio.

Para habilitar las nuevas características forest-wide, todos los Domain Controllers en el forest deberán correr Windows Server 2003, y el nivel funcional del forest se debe elevar a Windows Server 2003. Usted debe ser Enterprise Administrator para elevar el nivel funcional del forest.

Para obtener mas información acerca de niveles de funcionalidad:

http://support.microsoft.com/default.aspx?scid=kb;en-us;322692

5.4.2 Práctica 4: ¿Cómo elevar el nivel funcional?

Elevar la funcionalidad del forest y del dominio a Windows Server 2003 habilita ciertas características, por ejemplo, forest trusts, que no está disponible en otros niveles funcionales. Usted puede elevar la funcionalidad del forest y del dominio usando Active Directory Domains and Trusts.

Para elevar el nivel funcional del dominio, debe realizar los siguientes pasos:

1. Abrir Active Directory Domains and Trusts.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

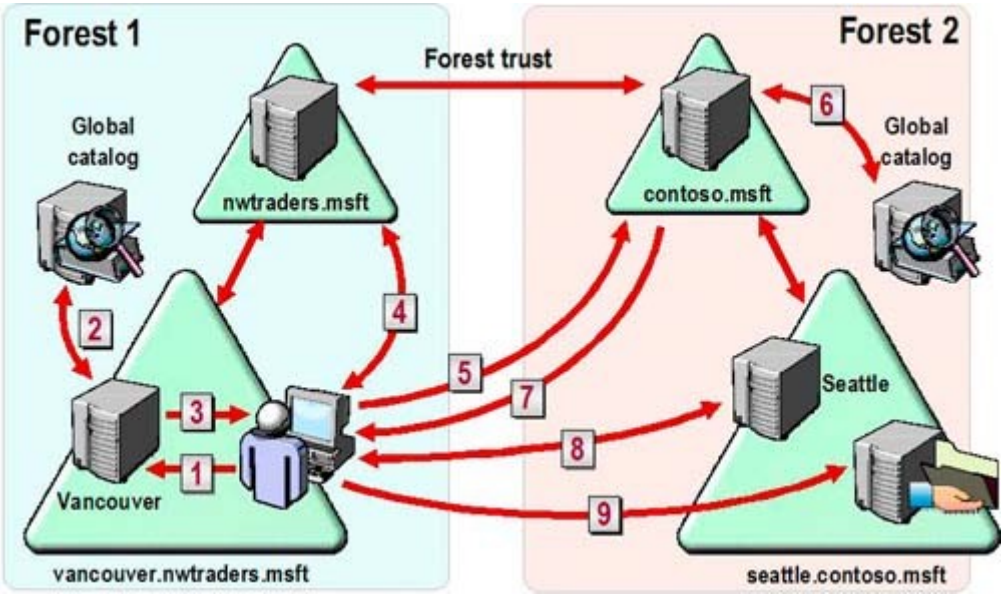
2. Hacer click derecho en la consola, en el nodo para el nivel funcional de dominio que usted desea elevar, y después hacer click en ***Raise Domain Functional Level***.
3. Seleccionar el nivel funcional Windows Server 2003 en el cuadro ***Select an available domain functional level***, y después hacer click en ***Raise***.

Para elevar el nivel funcional del forest, deberá realizar los siguientes pasos:

1. En Active Directory Domains and Trusts, en la consola, hacer click derecho en ***Active Directory Domains and Trusts***, y después click en ***Raise Forest Functional Level***.
2. En el cuadro ***Select an available forest functional level***, seleccionar ***Windows Server 2003***, y después hacer click en ***Raise***.

Nota: Usted debe elevar el nivel funcional de todos los dominios en un forest a Windows 2000 native o más alto, antes de elevar el nivel funcional del forest.

6. ¿Cómo funcionan los Trusts entre Forests?



6.1. Introducción

Windows Server 2003 soporta cross-forest trusts, el cual permite que los usuarios en un forest tengan acceso a recursos en otro forest. Cuando un usuario intente tener acceso a un recurso en un trusted forest, Active Directory primero localizará el recurso.

Después de localizar el recurso, el usuario podrá ser autenticado y tener acceso al recurso. Entender cómo este proceso trabaja, le ayudará a localizar problemas que pueden presentarse con cross-forest trusts.

6.2. ¿Cómo es accedido un recurso?

Lo que sigue es una descripción de cómo un cliente Windows 2000 Professional o Windows XP Professional localiza y tiene acceso a un recurso en otro forest que tenga Windows 2000 Server o Windows Server 2003 server.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

1. Un usuario que inicia sesión al dominio vancouver.nwtraders.msft intenta tener acceso a una carpeta compartida en el forest contoso.msft. La computadora del usuario contacta al KDC en un domain controller en vancouver.nwtraders.msft y solicita un service ticket usando el SPN de la computadora, donde reside el recurso. Un SPN puede ser el nombre de DNS de un host o dominio, o puede ser el Distinguished Name de un Service Connection Point Object.
2. El recurso no se encuentra en vancouver.nwtraders.msft y el Domain Controller de vancouver.nwtraders.msft realiza queries al Global Catalog para ver si el recurso está situado en otro dominio en el forest. Dado que el Global Catalog contiene solamente la información sobre su propio forest, no encuentra el SPN. El Global Catalog entonces comprueba su base de datos para saber si hay información sobre forest trusts establecidos con su forest. Si el Global Catalog encuentra uno, compara los name suffixes que están listados en el forest trust TDO para el suffix de destino SPN. Después de encontrar una igualdad, el Global Catalog proporciona la información de routing sobre cómo localizar el recurso al Domain Controller en vancouver.nwtraders.msft.
3. El Domain Controller en vancouver.nwtraders.msft envía una referencia para su dominio Parent, nwtraders.msft, a la computadora del usuario.
4. La computadora del usuario contacta al Domain Controller en nwtraders.msft por la referencia al Domain Controller del Forest Root Domain del forest contoso.msft.
5. Usando la referencia del Domain Controller en nwtraders.msft, la computadora contacta al Domain Controller en el forest contoso.msft para el pedido de servicio al service ticket.
6. El recurso no está situado en el Forest Root Domain del forest contoso.msft, y por eso el Domain Controller contacta a su Global Catalog para buscar el SPN. El Global Catalog busca el SPN y lo envía al Domain Controller.
7. El Domain Controller envía la referencia seattle.contoso.msft a la computadora del usuario.
8. La computadora del usuario contacta al KDC en el Domain Controller en seattle.contoso.msft y negocia el ticket para el acceso del usuario al recurso en el dominio seattle.contoso.msft.
9. La computadora envía el server service ticket a la computadora en la cual está el recurso compartido, donde se leen las credenciales de seguridad del usuario y se construye el access token, que da el acceso de usuario al recurso.

Nota: Recuerde que para poder utilizar esta nueva característica, debe tener los dos forest en nivel Windows Server 2003. Los trust entre forest en Windows Server 2003 le permiten validar usuarios usando Kerberos v5, utilizando la seguridad propia del protocolo. También le permite que los trust sean transitivos entre dos forest, no así, en múltiples forest. Por ejemplo: El forestA tiene establecido un trust con el forest B, y todos los dominios en los dos forest pueden utilizar el trust. Pero si a su vez el forest B tiene un trust con el forest C, no existe ningún tipo de relación entre el forest A y el forest C.

Para obtener más información acerca de trust:

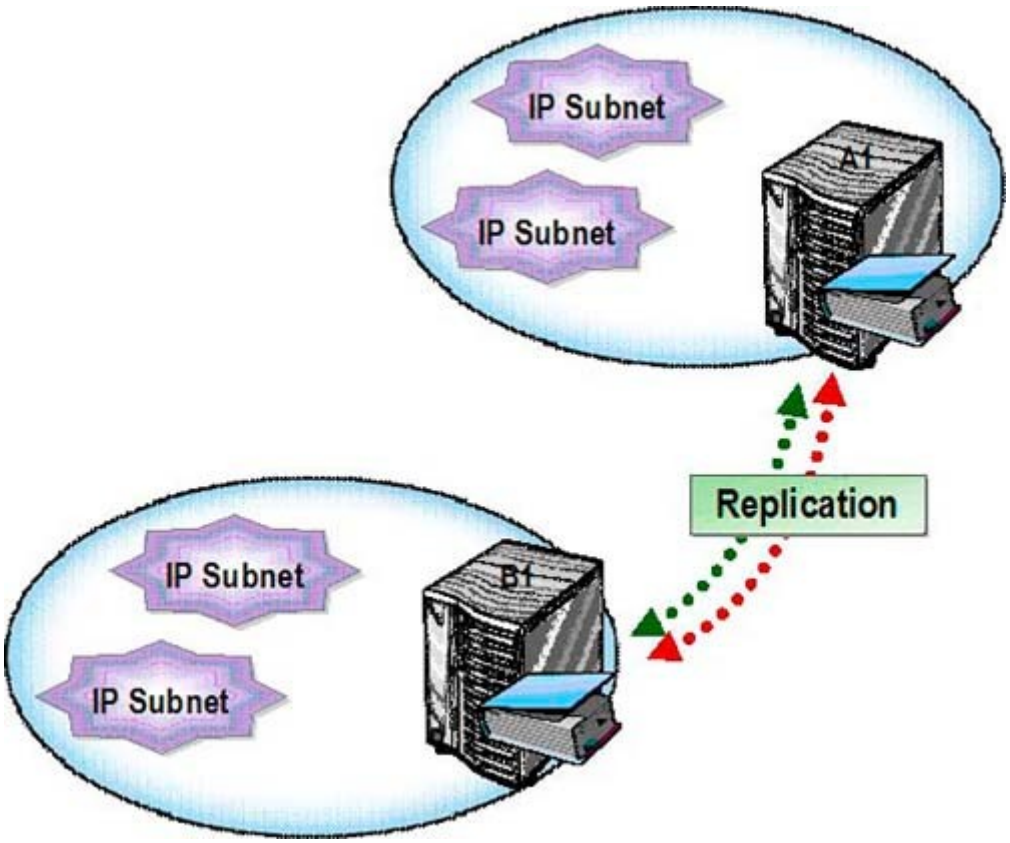
http://support.microsoft.com/default.aspx?scid=kb;en-us;325874

http://support.microsoft.com/default.aspx?scid=kb;en-us;816301

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio

7. Replicación en Active Directory



7.1. Replicación dentro de Sites

Los puntos dominantes de la replicación de Active Directory dentro de site son:

- ***La replicación ocurre cuando hay:***
  - Una adición de un objeto a Active Directory.
  - Una modificación de los valores de un atributo de objeto.
  - Un cambio de nombre de un contenedor de objetos.
  - Una eliminación de un objeto del directorio.

- ***Change notification.*** Cuando un cambio ocurre en un domain controller, el domain controller notifica a sus replication partners en el mismo site. Este proceso se llama change notification.

- ***Replication latency.*** Retrasa entre el tiempo que ocurre un cambio y el tiempo que la actualización alcanza a todos los Domain Controllers en el site. Por defecto la Replication Latency es 15 segundos.

- ***Urgent replication.*** En lugar de esperar los 15 segundos por defecto, los atributos sensibles de seguridad que se actualizan disparan un inmediato mensaje de change notification.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

- ***Convergence.*** Cada actualización en Active Directory eventualmente propaga a todos los Domain Controllers en el site que contiene la partición en la cual la actualización fue hecha. Esta propagación completa se llama convergence.

- ***Propagation dampening.*** El proceso de prevenir la réplica innecesaria. Cada Domain Controller asigna a cada cambio de atributo y objeto un Update Sequence Number (USN) para prevenir la réplica innecesaria.

- ***Conflicts.*** Cuando actualizaciones concurrentes que originan en dos réplicas master separadas son inconsistentes, los conflictos pueden presentarse. Active Directory resuelve tres tipos de conflictos: atributo, Contenedores eliminados, y conflictos de Relative Distinguished Name (RDN).

- ***Globally unique stamp.*** Active Directory mantiene un stamp que contiene el version number, timestamp, y server globally unique identifier (GUID) que Active Directory creado durante la actualización originaria.

7.2. new! Linked Multivalued Attributes

El proceso por el cual linked multivalued attributes se replican varía, dependiendo del nivel funcional del forest:

Cuando el nivel funcional del forest es menor que Windows Server 2003, cualquier cambio que fuera realizado a un atributo de miembros de grupo dispara la réplica de la lista entera del atributo miembro. El multivalued **member** attribute se considera un solo atributo con el fin de la réplica en este caso. Esta réplica aumenta la probabilidad de sobreescribir un cambio del atributo miembro que otro administrador realizó en otro domain controller, antes que el primer cambo fuera replicado.

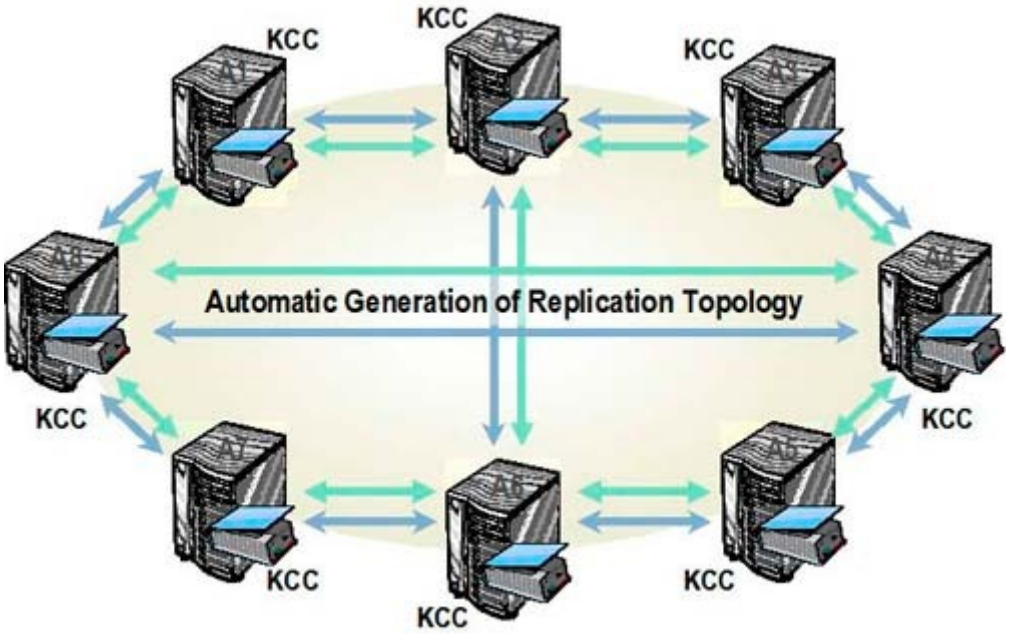
Cuando el nivel funcional del forest se cambia a Windows Server 2003, un valor individual replica cambios a linked multivalued attributes. Esta funcionalidad mejorada replica solamente cambios del atributo miembro de grupo y no a la lista entera del atributo de miembro.

De esta forma se elimina la restricción de 5000 usuarios máximo por grupo, esta restricción estaba dada en Windows 2000 por el valor máximo que puede tener el atributo de miembros de un grupo.

7.3. new! Generación automática de la topología de replicación

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio.com



Cuando usted agrega Domain Controllers a un site, Active Directory usa el Knowledge Consistency Checker (KCC) para establecer una trayectoria de la réplica entre Domain Controllers.

El KCC es un proceso que funciona en cada Domain Controller y genera la topología de la réplica para todas las particiones del directorio que se contengan en ese Domain Controller. El KCC corre en los intervalos específicos cada 15 minutos por defecto y diseña las rutas de replicación entre Domain Controllers de las conexiones más favorables que están disponibles en ese momento.

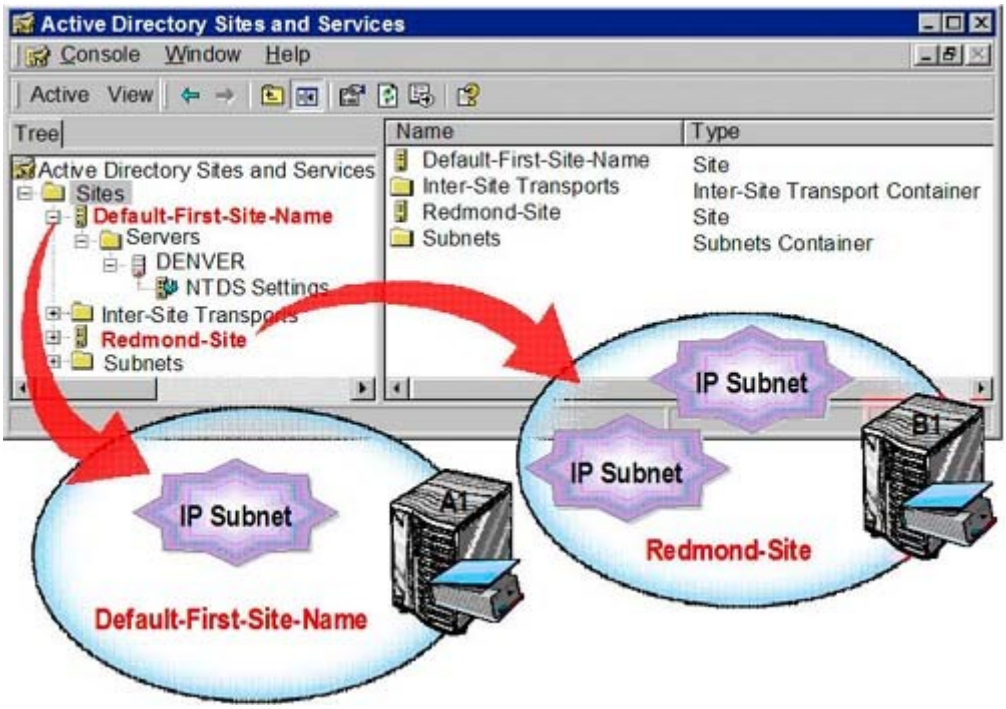
Este proceso fue mejorado con respecto al proceso de Windows 2000, haciendo que esta nueva característica elimine la limitación existente de un máximo de 500 sites en Active Directory. Actualmente se ha probado hasta 3000 sites y el soporte máximo es de 5000 sites.

Nota: Para aprovechar esta característica usted debe tener el forest en nivel funcional Windows Server 2003 ó Windows Server 2003 Interim.

7.4. Creando y Configurando Sites

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by



Usted utiliza sites para controlar el tráfico de replicación, tráfico de logon y las queries del cliente al Global Catalog Server.

7.4.1. ¿Qué son los sites?

En Active Directory, los sites ayudan a definir la estructura física de una red. Una o más subnets TCP/IP en una rango definido de direcciones define un site, el cual define alternadamente un grupo de Domain Controllers que tienen velocidad y costo similares. Los Sites consisten en objetos server, que contienen objetos de conexión que permiten la réplica.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

7.4.2. ¿Qué son objetos subnet?

Los objetos subnet identifican las direcciones de red las cuales utilizan las computadoras en los sites. Una subnet es un segmento de una red TCP/IP a la cual se asigna un sistema de direcciones lógicas IP. Dado que objetos subnet representan la red física, éstos hacen sites. Por ejemplo, si tres subnets están situados en tres campus en una ciudad, y estos campus están conectados con high-speed, conexiones altamente disponibles, usted podría asociar cada una de esas subnets a un site. Un site puede consistir en una o más subnets. Por ejemplo, en una red que tiene tres subnets en Redmond y dos en París, usted puede crear un site en Redmond, un site en Paris, y entonces agregar las subnets a los sites respectivos.

7.4.3. ¿Qué son los Site Links?

Los Site Links son conexiones que usted puede hacer entre sites para:

- Habilitar la replicación
- Manejar los horarios en los cuales usted quiere replicar,
- Mmanejar un costo de acuerdo al enlace que este utilizando, y el protocolo de replicación IP (RPC) o SMTP.

Para obtener mas información acerca de sites:

http://support.microsoft.com/default.aspx?scid=kb;en-us;323349

7.4.4 Práctica 5: Creando y Configurando Sites y Subnets

Para crear un site, deberá realizar los siguientes pasos:

1. Abrir Active Directory Sites and Services del menu ***Administrative Tools***.
2. Hacer click derecho en ***Sites*** en la consola, y después hacer click en ***New Site***.
3. Ingresar el nombre del nuevo site en el cuadro ***Name***.
4. Hacer click en un site link object, y después hacer click en ***OK*** dos veces.

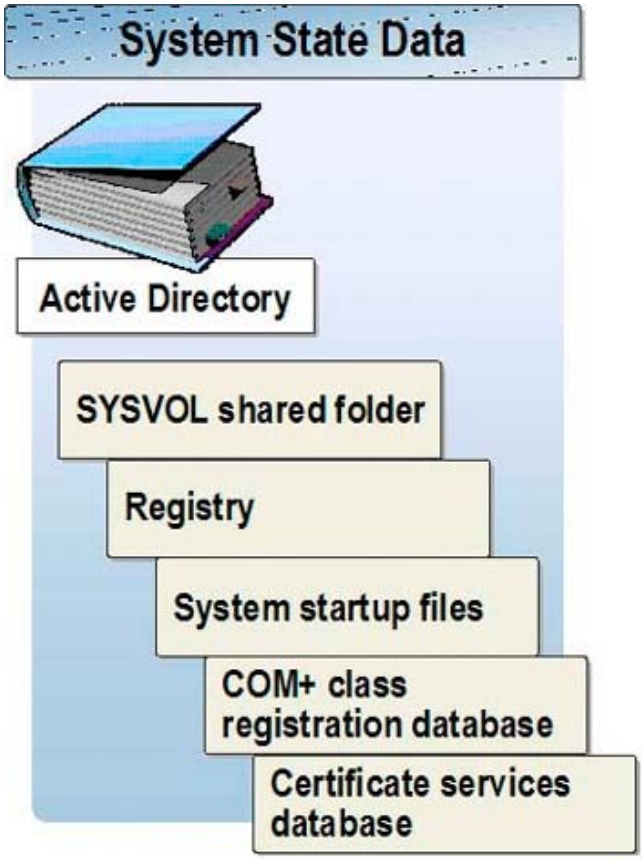
Para crear un subnet object, deberá realizar los siguientes pasos:

1. En Active Directory Sites and Services, en la consola, hacer doble-click en ***Sites***, hacer click derecho en ***Subnets***, y después hacer click en ***New Subnet***.
2. En el cuadro ***Address***, ingresar la dirección IP de la subnet.
3. En el cuadro ***Mask***, ingresar la subnet mask que describe el rango de direcciones de la subnet.
4. Seleccionar el site a asociar con la subnet, y después hacer click en ***OK***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

8. Haciendo backup de Active Directory



Hacer backup de Active Directory es esencial para mantener la base de datos de Active Directory. Usted puede hacer backup de Active Directory usando una graphical user interface (GUI) y herramientas command-line tools, que provee Windows Server 2003.

Usted con frecuencia debe hacer backup del System State data en Domain Controllers de modo que pueda restaurar los datos más actuales. Estableciendo un schedule regular de backup, Usted tiene una mejor ocasión de recuperación de datos cuando sea necesario.

El System State Data en un Domain Controller incluye los siguientes componentes:

Active Directory. El System State Data no contiene Active Directory a menos que el servidor en el cual Usted está haciendo backup del System State Data sea un Domain Controller. Active Directory está presente solamente en Domain Controllers.
The SYSVOL shared folder. Esta carpeta compartida contiene plantillas de Group Policy y logon scripts. La carpeta compartida SYSVOL está presente solamente en domain controllers.
The registry. Este repositorio base de datos contiene la información sobre la configuración de la computadora.
System startup files. Windows Server 2003 requiere estos archivos durante su fase de encendido inicial. Incluyen los boot y archivos de sistema que están protegidos por Windows file protection.
The COM+ Class Registration database. La base de datos Class Registration contiene información sobre Component Services applications.
The Certificate Services database. Esta base de datos contiene los certificados del servidor que Windows Server 2003 utiliza para autenticar usuarios. Esta base solamente está presente si el servidor está funcionando como certificate server.

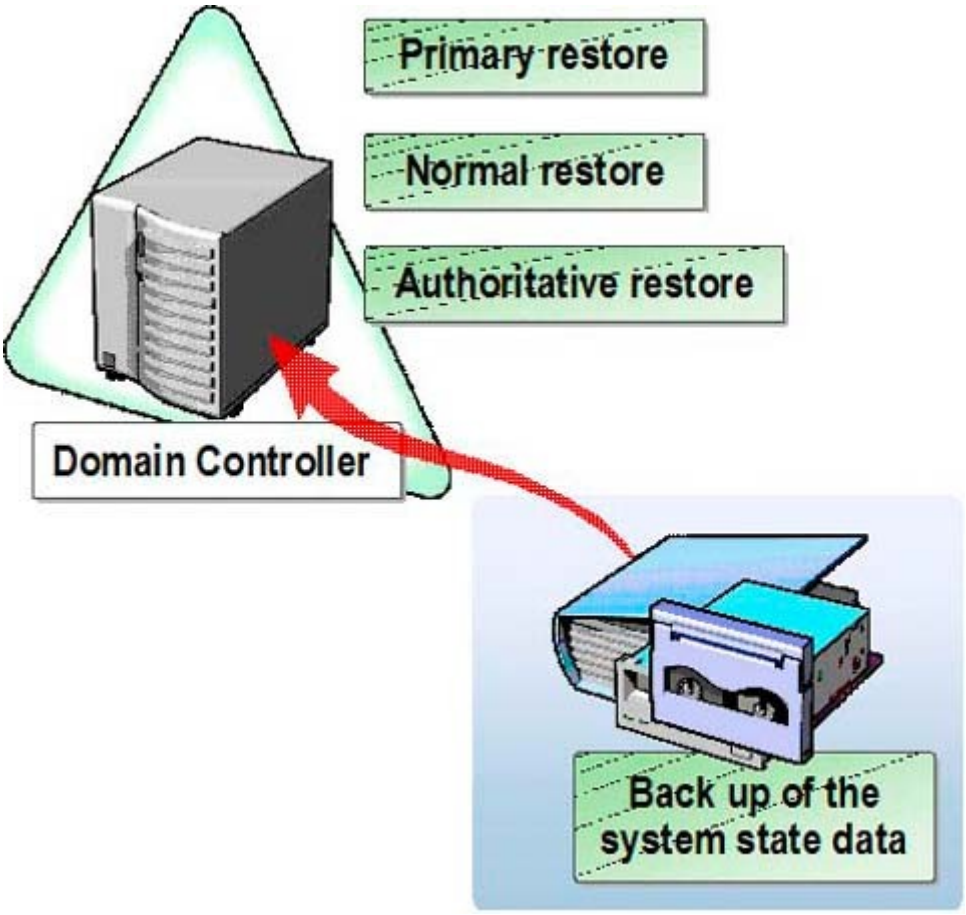
© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Para realizar la operación de backup usted puede utilizar la herramienta provista por Windows Server 2003:

1. Hacer click en ***Backup*** en el menu ***Start***, ***All Programs***, ***Accessories***, ***System Tools***.
2. Hacer click en ***Next*** en la página ***Welcome to the Backup or Restore Wizard***.
3. En la página ***Backup or Restore***, hacer click en ***Backup files and settings***, y después hacer click en ***Next***.
4. En la página ***What to Back Up***, hacer click en ***Let me choose what to back up***, y después hacer click en ***Next***.
5. En la página ***Items to Back Up***, expandir ***My Computer***, seleccionar el ***System State***, y después hacer click en ***Next***.
6. En la página ***Backup Type, Destination, and Name***, hacer click en ***Browse***, seleccionar una locación para el backup, hacer click en ***Save***, y después hacer click en ***Next***.
7. En la página ***Completing the Backup or Restore Wizard***, hacer click en ***Finish***.
8. En la página ***Backup Progress***, hacer click en ***Close***.

8.1 Restauración de Active Directory



© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by

Usted puede utilizar uno de los tres métodos para restaurar Active Directory de medios de backup: primary restore, normal (nonauthoritative) restore, y authoritative restore.

1. ***Primary restore.*** Este método reconstruye el primer domain controller en el dominio cuando no hay otra manera de reconstruir el dominio. Realizar un primary restore solamente cuando todos los domain controllers en un domain se perdieron, y usted desea reconstruir el dominio usando el backup.

2. ***Normal restore.*** Este método reinstala los datos de Active Directory al estado antes del backup, actualiza los datos con el proceso normal de réplica. Realizar un normal restore solamente cuando usted desea restaurar un solo domain controller a un buen estado previamente conocido.
3. ***Authoritative restore.*** Usted realiza este método en tándem con un restore normal. Un restore autoritativo marca datos específicos y evita que la réplica sobreescriba esos datos. Los datos autoritativos entonces se replican a través del dominio.

Para realizar un primary restore de Active Directory, deberá realizar los siguientes pasos:

1. Reiniciar su domain controller en Directory Services Restore Mode.
2. Iniciar la utilidad de Backup.
3. Hacer click en ***Advanced Mode*** en la página ***Welcome to the Backup or Restore Wizard***,
4. En la página ***Welcome to Backup Utility Advanced Mode***, sobre ***Restore and Manage Media***, seleccioar qué desea restaurar, y después hacer click en ***Start Restore***.
5. En el cuadro ***Warning***, hacer click en ***OK***.
6. En el cuadro ***Confirm Restore***, hacer click en ***Advanced***.
7. En el cuadro ***Advanced Restore Options***, hacer click en ***When restoring replicated data sets, mark the restored data as the primary data for all replicas***, y después hacer click en ***OK*** dos veces.
8. En el cuadro ***Restore Progress***, hacer click en ***Close***.
9. En el cuadro ***Backup Utility***, hacer click en ***Yes***.

© 2003 Microsoft Corporation. Todos los derechos reservados. Terminos de Uso

Powered by itsitio.com